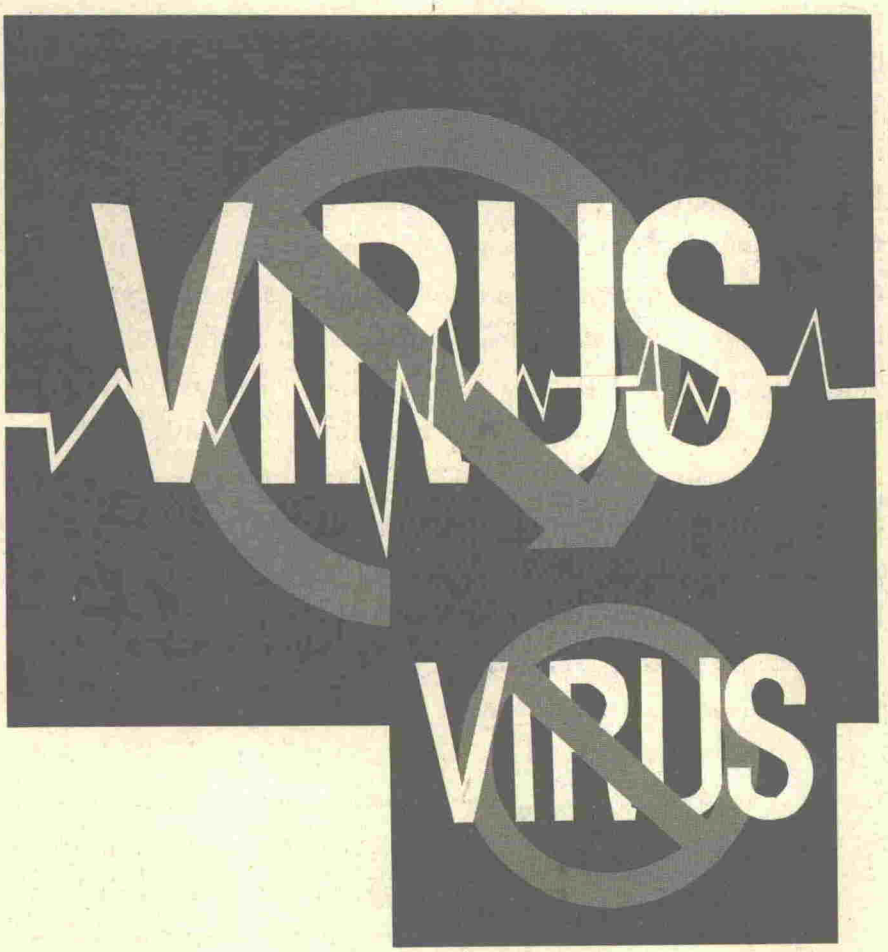
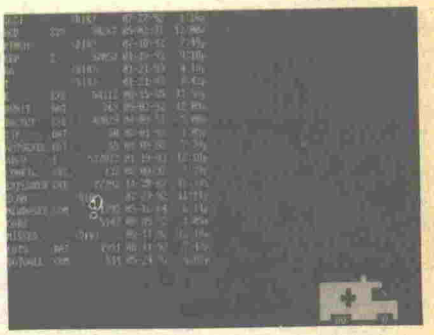
เรื่องน่าอ่าน
ทศเทพ บุญสิลา

15 เรื่องเบื้องหลัง ไวรัสคอมพิวเตอร์



ตามดูความเป็นมาของไวรัสศัตรูตัวฉกาจในเครื่องคอมพิวเตอร์

ไวรัสคอมพิวเตอร์เป็นที่รู้จักกันดีในหมู่ผู้ใช้คอมพิวเตอร์ทั่ว ๆ ไป บางท่านอาจจะเคยประสบพบเจอด้วยตัวเองจนเป็นที่คุ้นเคยกันดี ทำให้เราปวดหัวมาก็เยอะ จนต้องหาวิธีปราบปรามให้สิ้นซาก เรานำเกร็ดน่ารู้เล็ก ๆ น้อย ๆ ที่เกี่ยวกับไวรัสคอมพิวเตอร์มาฝากท่านผู้อ่านกันครับ



รูปที่ 1 ไวรัสที่ชื่อ Ambulance จะสร้างรถพยาบาลวิ่งบนจอภาพเมื่อมันปฏิบัติการ

01 ไวรัสคอมพิวเตอร์บางตัวก่อให้เกิดผลให้เราเห็นกันได้อย่างชัดเจน ตัวอย่างเช่น เจ้าไวรัสที่เรียกว่า รถพยาบาล (Ambulance) ซึ่งเมื่อมันทำงานจะเห็นเป็นรูปภาพรถพยาบาลวิ่งบนจอภาพอย่างชัดเจน พร้อมกับมีเสียงไซเรนให้เราฟังอีกด้วย มีบางคนได้นำเจ้าไวรัสนี้ไปดัดแปลงจนมีรถพยาบาลวิ่งทุกครั้งเมื่อรันโปรแกรมที่มีไวรัสนี้ฝังตัวอยู่ แต่ยังมีผู้นำเอาไวรัสรถพยาบาลไปดัดแปลงต่ออีกโดยให้วิ่งไปบนจอภาพแล้วชนกำแพงอิฐจนระเบิด เล่นกันจนสนุกมือเลย

02 ไวรัสตัวแรกสำหรับเครื่องพีซีก็คือ VIRDEM (เวอร์เดม) ถูกเขียนขึ้นเพื่อแสดงในการประชุม the Chaos Computer Club ในปีค.ศ. 1986 โดยนายราล์ฟ เบอร์เกอร์ และต่อมานายราล์ฟ เบอร์เกอร์ ก็ได้ผลิตซอฟต์แวร์ต่อต้านไวรัสออกมาให้ได้ใช้กัน ขอบคุณนะราล์ฟ

03 ไวรัสที่พบบ่อยที่สุดในยุโรปก็คือ Form เพราะเนื่องมาจากไวรัสตัวนี้ได้เกิดโชคดีที่บังเอิญได้เข้าไปอยู่ในขบวนการผลิตของผู้ผลิตซอฟต์แวร์รายใหญ่บริษัทหนึ่ง เลยทำให้มันถูก

ส่งออกไปพร้อม ๆ กับซอฟต์แวร์ที่ผลิตออกมาด้วย ไวรัส Form นี้มีถิ่นกำเนิดในสวิตเซอร์แลนด์ ซึ่งในจำนวนไวรัสที่ถูกค้นพบแล้วได้รับรายงานเข้ามาเป็นจำนวนถึง 90 เปอร์เซ็นต์ก็คือ เจ้า Form ตัวนี้นั่นเอง

04 ไวรัสนั้นมีทั้งที่ทำงานแบบซับซ้อน และที่ทำงานแบบง่าย ๆ ไวรัสที่ปฏิบัติการอย่างง่ายที่สุด มีความยาวของตัวมันเองเพียง 25 ไบต์เท่านั้น มันจะปฏิบัติการได้เพียงอย่างเดียวคือ การเขียนทับไฟล์หนึ่ง ๆ ด้วยตัวของมันเอง เจ้าไวรัสตัวนี้จึงถูกเรียกว่า TRIVIAL.25

05 ในจำนวนไวรัสกว่า 2,500 ชนิดที่เคยถูกค้นพบมา มีไวรัสอยู่ราว ๆ 50 ชนิดที่ถูกพบเห็นในโลกคอมพิวเตอร์จริง ๆ และมีไวรัสเพียง 20 ชนิดที่ถูกรายงานการค้นพบรวมแล้วเป็น 99 เปอร์เซ็นต์ของการรายงานการพบเจอไวรัสทั้งหมด แต่ถึงกระนั้นไม่มีใครจะทำนายได้ว่าไวรัสตัวไหนจะเกิดโชคดีเป็นเหมือนเจ้า Form ขึ้นมาอีก

06 มี BBS (Bulletin Board System) จำนวน 30 บอร์ดทั่วโลกที่เปิดให้ผู้ใช้บริการทำการแลกเปลี่ยนไวรัสที่หายาก และแปลกประหลาด ซึ่งผู้ใช้บริการบอร์ดนี้ทำการแลกเปลี่ยนไวรัสหายากและประหลาดเหมือนการสะสมแสตมป์เลยทีเดียว ผู้สะสมส่วนใหญ่ไม่ค่อยจะรู้ว่าไวรัสที่สะสมไว้นั้นเป็นไวรัสประเภทใด ชนิดใด และบางคนก็ไม่ค่อยรู้ว่าจะสะสมไปทำไมด้วย

07 สถาบันเพื่อการป้องกันไวรัสของอังกฤษ The Computer Crime Unit ได้ประกาศว่าไวรัส Brain ได้สูญพันธุ์ไปแล้ว แต่อย่างไรก็ตาม ยังมีผู้พบเจอเจ้าไวรัสตัวนี้ และได้รับการรายงานว่าพบเจอเจ้าไวรัส Brain เข้ามาอยู่เรื่อย ๆ

08 นายราล์ฟ เบอร์เกอร์ ได้พิมพ์หนังสือเล่มหนึ่ง ซึ่งประกอบด้วยวิธีการและการแยกชิ้นส่วนต่าง ๆ ของเจ้าไวรัสชื่อ เวียนนา (Vienna) ต่อมาไม่นานนัก ผลลัพธ์ที่ได้จากการจำหน่ายหนังสือเล่มนี้ก็คือ การค้นพบเวอร์ชันใหม่ ๆ ของเจ้าเวียนนากว่า 100 เวอร์ชันออกมาระบาดกันทั่วเมือง ไวรัสที่ถูกลอกเลียน และดัดแปลงมากเป็นอันดับสองรองลงมาก็คือ Jerusalem และอันดับที่สามก็คือ Stone

09 ไวรัสที่ถูกตรวจจับได้ยากที่สุดก็เห็นจะเป็นไวรัสจำพวก polymorphic ซึ่งเป็นไวรัสที่ถูกเขียนขึ้นโดย the Dark Avenger Mutation Engine หรือ the Trident Polymorphic engine มีเพียงซอฟต์แวร์ต่อต้านไวรัสบางส่วนเท่านั้นที่สามารถตรวจพบไวรัสจำพวกนี้ ซึ่งซอฟต์แวร์ส่วนใหญ่ไม่สามารถตรวจพบเลย

10 ไวรัสจำพวก polymorphic ตัวแรกถูกเขียนขึ้นโดยนายมาร์ค วอช-เบอร์น เขาต้องการที่จะแสดงให้เห็นว่า สามารถเขียนไวรัสที่ไม่มีการเรียงตัวของไบต์ในตัวของมันที่แน่นอน หรืออีกนัยหนึ่งก็คือ ตัวของมันเองจะเปลี่ยนแปลงไปเรื่อย ๆ นั่นเอง จึงทำการตรวจจับโดยการใช้วิธีการเปรียบเทียบหาแพตเทอร์นนั้นทำได้ยาก นายวอชเบอร์นใช้ไวรัสเวียนนาเป็นพื้นฐานในการเขียนแต่ทำการเรียบเรียงใหม่โดยให้มีการก๊อบปี้ตัวเองในตัวต่อไปไม่ให้เหมือนกับตัวเดิมของมัน หรือให้ลูกหลานของมันมีแพตเทอร์นของไบต์ที่ต่างกันออกไป ซึ่งเขาได้เขียนไวรัสจำพวกนี้ออกมามากมายหลายรุ่น ซึ่งเรา ๆ ท่าน ๆ อาจจะได้พบเจอกันไปแล้วบ้าง ใครจะไปรู้ได้

11 ความเสียหายที่ร้ายแรงที่สุดจากการทำลายของไวรัส ไม่ได้เกิดจากการปฏิบัติการของไวรัสชนิดที่ทำการฟอร์แมตฮาร์ดดิสค์ของท่านถึงขั้นโลว์เลเวล แต่ความเสียหายที่รุนแรงมากกว่านั้น เกิดจากไวรัสพวกที่ทำการเปลี่ยนแปลงข้อมูลของท่านอย่างช้า ๆ และเงียบเชียบ โดยที่ท่านไม่รู้ตัว เมื่อท่านรู้สึกตัวก็ไม่รู้ว่าจะนำเอาแบคอัพตัวไหนมาใช้ เพราะไม่รู้ว่าเริ่มได้รับเชื้อไวรัสเข้ามาเมื่อใด

ไวรัสส่วนมากจะทำความเสียหายให้กับคอมพิวเตอร์ไม่มากเท่าไร ผู้ใช้คอมพิวเตอร์ต่างหากที่ทำความเสียหายให้กับตัวเอง โดยการพยายามกำจัดไวรัสซึ่งฝังตัวอยู่ในฮาร์ดดิสค์หรือในฟลอปปี้ดิสค์ ความเสียหายนี้อาจจะมากกว่าผลที่เกิดจากการทำลายของเจ้าไวรัสเองเสียอีก การฟอร์แมตแบบโลว์เลเวลนั้นพบกันได้ทั่วไปในไวรัสต่าง ๆ แต่ผู้ใช้บางคนตัดสินใจที่จะเปลี่ยนฮาร์ดดิสค์เพื่อเป็นการกำจัดไวรัส ดูซิว่าการพยายามกำจัดไวรัสซึ่งฝังตัวอยู่ในฮาร์ดดิสค์กับการเปลี่ยนฮาร์ดดิสค์ใครทำความเสียหายมากกว่ากัน

12 ในประเทศอังกฤษมีการตั้งคลีนิกไวรัสขึ้นมา แต่มิใช่เพื่อการรักษาหรือป้องกันการแพร่ระบาดของเจ้าไวรัส คลีนิกดังกล่าวตั้งขึ้นเพื่อขายไวรัสให้กับคนทั่วไป และมีการโปรโมทกันมาก

จนถึงขั้นนำไปลงในโฆษณาในวารสารคอมพิวเตอร์ฉบับหนึ่ง หลังจากนั้นไม่ถึงหนึ่งอาทิตย์ เจ้าหน้าที่ตำรวจก็ได้เข้าไปทำการปิดคลีนิกไวรัสดังกล่าวลง และทำการดำเนินคดีตามกฎหมายกับเจ้าของคลีนิก

13 ผู้เขียนไวรัสที่ชื่อ ตากีลา (Tequila) ได้เขียนที่อยู่ของเขาลงในไวรัส แต่เป็นที่น่าเสียดายที่ประเทศสวิตเซอร์แลนด์ไม่มีกฎหมายต่อต้านการกระทำดังกล่าว จึงไม่สามารถดำเนินคดีกับผู้เขียนซึ่งเป็นชาวสวิตซ์ได้ ส่วนในไวรัส Brain เวอร์ชันหนึ่ง ได้มีการบรรจุหมายเลขโทรศัพท์ 3 เลขหมาย แต่หลังจากการตรวจสอบพบว่าเป็นหมายเลขซึ่งไม่มีใครเป็นเจ้าของ

14 ไวรัสที่มีโครงสร้างซับซ้อนเยอะ ตรวจจับได้ยากทั้งหลายนั้น ถูกเขียนขึ้นในประเทศต่าง ๆ เช่น บูลแกเรีย โปแลนด์ เชคโกสโลวาเกีย และรัสเซีย และในขณะนี้ฮอลแลนด์ก็กำลังจะเลื่อนตำแหน่งเข้ามาอยู่ในกลุ่มนี้ด้วย ในขณะที่อเมริกามุ่งในการผลิตที่เป็นอุตสาหกรรม โดยมีผู้เขียนซอฟต์แวร์แพคเกจเพื่อช่วยในการผลิตไวรัสได้มากขึ้น ไวรัสที่ถูกผลิตออกมาจะเป็นไวรัสในตระกูลเดียวกัน แต่จะมีลักษณะเด่น ๆ แตกต่างกันออกไป

15 ในประเทศอังกฤษได้มีกลุ่มผู้ผลิตไวรัสเกิดขึ้นชื่อว่า ARCV ซึ่งเป็นกลุ่มที่รวมตัวกันเพื่อการผลิตไวรัสออกมาให้ระบาดโดยเฉพาะ กลุ่มนี้ได้ผลิตไวรัสออกมา 20 กว่าชนิด แต่เป็นชนิดที่ปฏิบัติการง่าย ๆ ไม่ซับซ้อนมากนัก ในขณะที่เจ้าหน้าที่ตำรวจก็กำลังสืบหาแหล่งที่กลุ่มนี้รวมตัวกันอยู่

ตารางที่ 1
แสดงตัวอย่างของไวรัสซึ่งมีบักอยู่ด้วย

ไวรัสก็มีบัก

ไวรัสหลายตัวมีบักในตัวมันเอง และนี่เป็นตัวอย่างของไวรัสซึ่งมีบักอยู่ด้วย

★ ไวรัสหลายชนิด มีอาการในการทำฟอร์แมตแบบโลว์-เลเวล ฟลอปปี้อันที่สาม ซึ่งส่วนมากจะไม่มีในเครื่องทั่วไป ทำให้เกิดเป็นข้อผิดพลาด (Error) นั่นก็เพราะผู้เขียนนึกว่าไดรฟ์นั้นเป็นฮาร์ดดิสค์ไดรฟ์

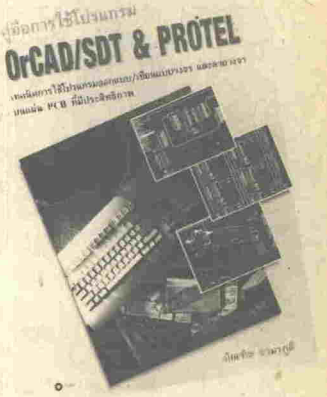
★ ไวรัสบางจำพวกใช้อินเตอร์รัพต์ 15h และอินเตอร์รัพต์ 0dh เมื่อความเป็นจริงผู้เขียนไวรัสตัวนั้นต้องการให้ใช้อินเตอร์รัพต์ 21 h และ 13 h ต่างหาก ทั้งนี้ก็เพราะผู้เขียนลืมใช้เลขเฮกซาเดซิมอลในการเขียนไวรัสนั่นเอง

★ ไวรัสที่ซับซ้อนมากที่สุดชื่อว่า Whale หรือเจ้าปลาวาฬ ซึ่งมีขนาด 9 กิโลไบต์ หรือประมาณ 90 เปอร์เซ็นต์ของโค้ด ใช้ในการทำให้จอภาพมืด และทำให้เกิดการเปลี่ยนแปลงต่าง ๆ เจ้าไวรัสตัวนี้ซับซ้อนมาก แค่ทำงานได้ไม่นานก็ทำให้เครื่องคอมพิวเตอร์เกิดการแฮงค์ไปเลย

ซีเอ็ด

เทคนิคการใช้โปรแกรม ออกแบบ/เขียนแบบวงจร และลายวงจรบนแผ่น PCB ที่มีประสิทธิภาพ

คู่มือการใช้โปรแกรม
OrCAD/SDT & PROTEL



โดย บัณฑิต จามรภูติ

งานทางด้านวิศวกรรมไฟฟ้าและอิเล็กทรอนิกส์ ส่วนมากจะเกี่ยวข้องอยู่กับการออกแบบวงจรหรือแบบ PCB ต่าง ๆ นักศึกษาระดับ ปวส. และปริญญาตรีก็ต้องใช้งานเกี่ยวกับวงจรอิเล็กทรอนิกส์ทั่วไป หรือการทำโปรแกรมขึ้นมาหนึ่งชิ้นจะต้องออกแบบวงจรก่อนทั้งสิ้น การออกแบบโดยใช้มือเขียนนั้นเป็นเพียงแบบร่างเอาไว้ แต่เมื่อจะนำเสนอเป็นมาตรฐาน จะต้องใช้โปรแกรมออกแบบวงจรแผ่น PCB เข้าช่วยให้ดูดีขึ้น

OrCAD และ Protel เป็นโปรแกรมออกแบบวงจรไฟฟ้าและอิเล็กทรอนิกส์ที่มีประสิทธิภาพ เป็นที่นิยมในเมืองไทยมาก การใช้งานง่ายและสะดวก แต่ส่วนมากจะใช้งานโปรแกรมเหล่านี้ไม่เต็มร้อยเปอร์เซ็นต์ เพราะไม่รู้วิธีใช้ที่เต็มประสิทธิภาพ "คู่มือการใช้โปรแกรม OrCAD/SDT & Protel" จะช่วยแนะนำเทคนิคต่าง ๆ ในการใช้งานโปรแกรมเหล่านี้ให้ดียิ่งขึ้น

วางตลาดแล้ว

หาซื้อได้ตามร้านหนังสือชั้นนำทั่วไป